Теорема 3. Пусть $1 \leqslant j < i \leqslant 2^n - 1$, $1 \leqslant k \leqslant 2^n - 1$, α — примитивный элемент поля $\mathbb{F}_{2^n}$. Если n — составное число, то существует взаимно однозначная функция $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ вида $f(x) = \alpha^k x^i + x^j$.

Опираясь на результаты [2], доказана

Теорема 4. Если $2^n - 1$ имеет делитель $d < \dfrac{n}{2\log_2(n)} - 1$, то существует взаимно однозначная функция $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ вида $f(y) = ay^i + y^j$ для некоторого $a \in \mathbb{F}^*_{2^n}$, $0 < j < i < 2^n - 1$.

Остался не исследованным вопрос существования взаимно однозначной векторной булевой функции при простом числе n и составном числе $2^n - 1$, если у него нет делителя $d < \dfrac{n}{2\log_2(n)} - 1$.

С использованием полученных результатов найдены все взаимно однозначные функции данного вида для всех $n \leqslant 8$. При этих же значениях n найдены все взаимно однозначные биномиальные дифференциально 4-равномерные векторные булевы функции. Посчитано количество взаимно однозначных биномиальных функций с максимальной компонентной алгебраической иммунностью при $n = 4, 6$. При $n = 4$ таких функций 10, а при $n = 6$ — 319 [3].

ЛИТЕРАТУРА

1. *Shallue C. J.* Permutation Polynomials of Finite Fields. Honours Thesis. Monash University, 2012.
2. *Masuda A. M. and Zieve M. E.* Permutation binomials over finite Ffeld // Trans. AMS. 2009. V. 361. No. 8. P. 4169–4180.
3. *Милосердов А. В.* Комбинаторные свойства полиномиального представления булевой функции. Выпускная квалификационная работа бакалавра. Новосибирск: НГУ, 2017.

УДК 519.7 DOI 10.17223/2226308X/10/19

НИЖНИЕ ОЦЕНКИ РАЗМЕРНОСТИ ЛИНЕЙНЫХ КОДОВ ДЛЯ ТЕХНОЛОГИИ СОТОВОЙ СВЯЗИ CDMA[1]

Н. С. Одинокиx

Линейный код называется *кодом, сохраняющим свойство бент* (*SPB-кодом*) для функции f, если сдвиг на любой элемент кода оставляет функцию f в классе бент-функций. В работе построены линейные SPB-коды для функций из класса Мэйорана — МакФарланда, получены нижние оценки максимальной размерности SPB-кодов для произвольной бент-функции.

Ключевые слова: *линейные коды, бент-функции, коды постоянной амплитуды.*

Code Division Multiple Access (CDMA) — это технология мобильной связи, основанная на кодовом разделении канала. Для оценки качества сигнала в CDMA вводится понятие коэффициента отношения пиковой и средней мощностей сигнала (Peak-to-Average Power Ratio). Многие задачи, связанные с CDMA, направлены на снижение коэффициента PAPR, так как высокие значения коэффициента ведут к необходимости использования дорогих усилителей. Векторами, на которых достигается минимальное

[1]Работа поддержана грантом РФФИ, проект № 17-41-543364.

значение PAPR, являются векторы значений бент-функций. В связи с этим возникает задача поиска кодов, состоящих из векторов значений бент-функций. Одним из способов построения таких кодов является построение линейного кода для некоторой бент-функции f, такого, что сдвиг на любую функцию из кода оставляет функцию f в классе бент-функций. Код длины 2^n называется *кодом постоянной амплитуды*, если все элементы кода являются векторами значений бент-функций. Линейный код длины 2^n называется *кодом, сохраняющим свойство бент* (*SPB-кодом*) для функции f, если сдвиг на любой элемент кода оставляет функцию f в классе бент-функций [1]. Если C — SPB-код, то его аффинный сдвиг $f \oplus C$ является кодом постоянной амплитуды. Это свойство позволяет конструировать коды постоянной амплитуды из линейных кодов.

В работе исследуются свойства бент-функций, лежащих в классе Мэйорана — МакФарланда [2]. Получена нижняя оценка максимальной размерности SPB-кода для произвольной бент-функции.

Теорема 1. Пусть f — бент-функция из класса Мэйорана — МакФарланда от $2n$ переменных. Тогда для функции f существует SPB-код размерности $2^{n+1} - 1$.

В [3] В. В. Ященко ввёл понятие *индекса линейности* для произвольной булевой функции. Любую булеву функцию можно представить в виде $f(x, y) = x_1\varphi_1(y) + \ldots + x_t\varphi_t(y) + \psi(y)$, $x \in \mathbb{F}_2^t$, $y \in \mathbb{F}_2^{n-t}$. Среди всех таких представлений есть представление с максимальным t, которое является аффинным инвариантом и называется индексом линейности булевой функции.

Теорема 2. Пусть f — бент-функция, индекс линейности которой равен k. Тогда для функции f существует SPB-код размерности $2^{k+1} - 1$.

ЛИТЕРАТУРА

1. *Павлов А. В.* Бент-функции и линейные коды в CDMA // Прикладная дискретная математика. Приложение. 2010. № 3. С. 95–97.
2. *McFarland R. L.* A family of difference sets in non-cyclic groups // J. Combin. Theory. Ser. A. 1973. V. 15. No. 1. P. 1–10.
3. *Ященко В. В.* О критерии распространения для булевых функций и о бент-функциях // Пробл. передачи информ. 1997. Т. 33. Вып. 1. С. 75–86.

УДК 519.212.2, 519.214 DOI 10.17223/2226308X/10/20

УТОЧНЁННЫЕ АСИМПТОТИЧЕСКИЕ ОЦЕНКИ ДЛЯ ЧИСЛА (n, m, k)-УСТОЙЧИВЫХ ДВОИЧНЫХ ОТОБРАЖЕНИЙ

К. Н. Панков

Уточнена локальная предельная теорема для распределения части вектора спектральных коэффициентов линейных комбинаций координатных функций случайного двоичного отображения. С помощью этой теоремы получена асимптотическая формула для $|R(m, n, k)|$ — числа (n, m, k)-устойчивых двоичных отображений в случае $n \to \infty$, $m \in \{1, 2, 3, 4\}$ и $k \leqslant \dfrac{n(1-\varepsilon)}{5 + 2\log_2 n}$ для произвольного $0 < \varepsilon < 1$, $k = \mathrm{O}\left(\dfrac{n}{\ln n}\right)$: